I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: June 10, 2008
Electronic Signature: /Jeffrey T. Gedeon/ (Jeffrey T. Gedeon)

Docket No.: 00-VE23.28
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Robert T. Baum

Application No.: 09/910,429 | Confirmation No.: 2654

Filed: July 20, 2001 | Art Unit: 2137

For: SECURITY EXTENSIONS USING AT LEAST A PORTION OF LAYER 2 INFORMATION OR BITS IN THE PLACE OF LAYER 2 INFORMATION | Examiner: M. J. Pyzocha

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This appeal is from the decision of the Primary Examiner dated September 11, 2006 ("Final Office Action") finally rejecting claims 1-24, 26-28 and 30-38, which are reproduced in an Appendix to this brief. A Notice of Appeal under 37 CFR §41.31 was filed on March 18, 2007. This application was filed on July 20, 2001. This brief is being filed concurrently with a petition to revive an unintentionally abandoned application.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application

II. RELATED APPEALS AND INTERFERENCES

Applicant (hereinafter "Appellant") is not aware of any related appeals or interferences that would affect the Board's decision on the current appeal.

III. STATUS OF CLAIMS

Claims 1-24, 26-28, 30-38 are pending and stand rejected, and are the subject of this appeal. Claims 25 and 29 were cancelled.

IV. STATUS OF AMENDMENTS

Appellant did not submit, and the Examiner did not enter, any amendments to the application subsequent to the Final Office Action dated September 11, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following summary of the presently claimed subject matter indicates certain portions of the specification (including the drawings) that provide examples of embodiments of elements of the claimed subject matter. It is to be understood that other portions of the specification not cited herein may also provide examples of embodiments of elements of the claimed subject matter. It is also to be understood that the indicated examples are merely examples, and the scope of the claimed subject matter includes alternative embodiments and equivalents thereof. References herein to the specification are thus intended to be exemplary and not limiting.

1. Claim 1

Independent claim 1 recites a method for authenticating a party to a transaction, the method comprising:

receiving (e.g., step 1810 in Fig. 18, page 36, lines 9-12) a packet having at least a part of layer 2 header information replaced with a unique bit string (e.g., bits 1520 in Fig. 16, page 30, lines 4-26);

examining at least a part of the unique bit string (e.g., step 1820 in Fig. 18, page 36, lines 12-14);

comparing the at least a part of the unique bit string examined with stored information (e.g., step 1840 in Fig. 18, page 37, lines 7-10); and

authenticating the party only if the at least a part of the unique bit string examined matches the stored information (e.g., step 1870, in Fig. 18, page 37, lines 17-25).

2. Claim 3

Claim 3 depends from claim 1 and further recites that at least a part of the unique bit string examined depends on a type of the transaction (e.g. step 1820 in Fig. 18, page 36, line 16 – page 37, line 5).

3. Claim 7

Claim 7 depends from claim 1 and further recites that at least a part of the unique bit string examined identifies a location at which packets from the party to the transaction entered the network (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10).

4. Claim 8

Claim 8 depends from claim 1 and further recites that at least a part of the unique bit string examined identifies an individual who is a party to the transaction (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23).

5. Claim 9

Claim 9 depends from claim 1 and further recites that at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23).

6. Claim 10

Claim 10 depends from claim 1 and further recites that at least a part of the unique bit string examined identifies a customer that is a party to the transaction (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23).

7. Claim 11

Claim 11 depends from claim 1 and further recites that at least a part of the unique bit string identifies at least one of a customer identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), an individual user identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), a network ingress location (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10), and a user class (e.g., service identifier 1320 in Fig. 13, page 26, lines 8-10).

8. Claim 12

Claim 12 depends from claim 1 and further recites that at least a part of the unique bit string identifies at least two of a customer identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), an individual user identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), a network ingress location (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10), and a user class (e.g., service identifier 1320 in Fig. 13, page 26, lines 8-10).

9. Claim 13

Claim 13 depends from claim 1 and further recites that at least a part of the unique bit string identifies at least three of a customer identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), an individual user identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), a network ingress location (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10), and a user class (e.g., service identifier 1320 in Fig. 13, page 26, lines 8-10).

10. Claim 16

Claim 16 depends from claim 1 and further recites that the act of authenticating does not require the transmission of any authentication information from the party (e.g., just a portion of the context information by itself, page 37, lines 26-32).

11. Claim 17

Independent claim 17 recites a method for tracking a network ingress location at which a packet associated with a transaction originated, the method comprising:

receiving (e.g., step 1810 in Fig. 18, page 36, lines 9-12) the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string (e.g., bits 1520 in Fig. 16, page 30, lines 4-26);

examining at least a part of the unique bit string (e.g., step 1820 in Fig. 18, page 36, lines 12-14); and

determining the network ingress location (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10) from the at least a part of the unique bit string (e.g., step 1870 in Fig. 18, page 36, lines 24-29, page 37, lines 17-25).

12. Claim 19

Claim 19 depends from claim 17 and further recites that at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23).

13. Claim 20

Claim 20 depends from claim 17 and further recites that at least a part of the unique bit string examined identifies a customer that is a party to the transaction (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23).

14. Claim 21

Claim 21 depends from claim 17 and further recites that at least a part of the unique bit string identifies at least one of a customer identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), an individual user identification (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23), a network ingress location (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10), and an individual user class (e.g., service identifier 1320 in Fig. 13, page 26, lines 8-10).

15. Claim 24

Independent Claim 24 recites a method for authenticating a party to a transaction, the method comprising:

receiving (e.g., step 1810 in Fig. 18, page 36, lines 9-12) a packet having at least a part of layer 2 header information replaced with a unique bit string (e.g., bits 1520 in Fig. 16, page 30, lines 4-26);

examining at least a part of the unique bit string (e.g., step 1820 in Fig. 18, page 36, lines 12-14);

comparing the at least a part of the unique bit string examined with stored information (e.g., step 1840 in Fig. 18, page 37, lines 7-10); and

approving a transaction only if the at least a part of the unique bit string examined matches the stored information (e.g., step 1870, in Fig. 18, page 37, lines 17-25), wherein the unique bit string uniquely identifies the party and an ingress location of the network (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10), and no information in addition to the unique bit string is needed for authenticating the party to the transaction (e.g., just a portion of the context information by itself, page 37, lines 26-32).

16. Claim 27

Claim 27 depends from claim 24 and further recites that the unique bit string identifies a logical port at which the packet entered the network (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10).

17. Claim 28

Independent Claim 28 recites a method for authenticating a party to a transaction, the method comprising:

a) applying (e.g., encapsulation process 1138 in Fig. 11, page 32, line 28 – page 33, line 9) a unique bit string to layer 2 header information of packets entering the network (e.g., bits 1520 in Fig. 16, page 30, lines 4-26), the unique bit string uniquely identifying the party (e.g., VPN-ID 1312 in Fig. 13, page 26, lines 12-23) and an ingress location of the network (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10);

b) examining at least a part of the unique bit string (e.g., step 1820 in Fig. 18, page 36, lines 12-14);

c) comparing the at least a part of the unique bit string examined with stored information (e.g., step 1840 in Fig. 18, page 37, lines 7-10); and

d) approving a transaction only if the at least a part of the unique bit string examined matches the stored information (e.g., step 1870, in Fig. 18, page 37, lines 17-25).

18. Claim 31

Claim 31 depends from claim 28 and further recites that the unique bit string identifies a logical port at which the packet entered the network (e.g., logical ingress port 1314 in Fig. 13, page 26, line 25 – page 27, line 10).

19. Claim 32

Claim 32 depends from claim 28 and further recites that no information in addition to the unique bit string is needed for authenticating the party to the transaction (e.g., just a portion of the context information by itself, page 37, lines 26-32).

20. Claim 33

Independent Claim 33 recites an apparatus for authenticating a party to a transaction, the apparatus comprising:

a) an input for accepting an authentication request (e.g., customer facing port 1130 in Fig. 11, page 32, lines 11-16), the authentication request including a packet having at least a part of a layer 2 header information replaced with a unique bit string (e.g., bits 1520 in Fig. 16, page 30, lines 4-26);

b) storage means for storing authentication information (e.g., tables in Fig. 11, page 32, lines 24-28);

c) means for examining at least a part of the unique bit string (e.g., step 1820 in Fig. 18, page 36, lines 12-14);

d) a comparison facility for comparing the at least a part of the unique bit string examined with the stored authentication information (e.g., step 1840 in Fig. 18, page 37, lines 7-10); and

e) means for authenticating a party to a transaction only if the at least a part of the unique bit string examined matches the stored authentication information (e.g., step 1870, in Fig. 18, page 37, lines 17-25).

21. Claim 38

Claim 38 depends from claim 17 and further recites that the layer 2 header information is a MAC header (e.g. bits 1520 in Fig. 16, page 30, lines 4-26).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-4, 6, 14-16, and 33-37 are patentable under 35 U.S.C. § 103(a) over Valencia et al, Cisco Layer Two Forwarding (Protocol) "L2F" (hereinafter "Valencia") in view of United States Patent 5,988,497 (hereinafter "Wallace").

2. Whether claims 5, 7-13, 17-24, 26-28, 30-32, and 38 are patentable under 35 U.S.C. § 103(a) over Valencia and Wallace in view of United States Patent 5,880,446 ("Mori").

VII. ARGUMENT

A. Ground of Rejection No. 1: Claims 1-4, 6, 14-16, and 33-37.

1. Obviousness.

With respect to the present Section 103 rejections, the Examiner has failed to meet the burden of stating a prima facie case of obviousness. The MPEP § 2143.01 summarizes the relevant case law as follows:

> The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art, and all teachings in the prior art must be considered to the extent that they are in analogous arts. Where the teachings of two or more prior art references conflict, the examiner must weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another. *In re Young*, 927 F.2d 588, 18 USPQ2d 1089 (Fed. Cir. 1991). (Emphasis added)

In the *KSR International Co. v. Teleflex, Inc.*, 550 U.S. ___, 127 S. Ct. 1727, 82 USPQ2d 1385 (April 30, 2007), the Supreme Court stated that

> it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.

Id. at 1396. The Court further explained that

> What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under §103. One of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims.

Id. at 1397. Accordingly, the Court made clear that "a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known and in the prior art." Id. at 1396. Here, the Examiner's rejections should be reversed because the cited

references do no teach or suggest any "known problem for which there was an obvious solution encompassed by the patent's claims."

In summary, *KSR* plainly does not disturb the well-settled proposition that a prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984); M.P.E.P § 2141.02. Further, the USPTO has published Section 103 Examination Guidelines providing seven rationales for claim rejections as examples of applications of *KSR* under Section 103, consistent with this requirement of *Gore*. *See Section 103 Examination Guidelines, 72 F.R. 57526 (October 10, 2007).*

2. Claim 1 Is Patentable Over Valencia In View Of Wallace.

Independent claim 1 recites in part "receiving a packet having at least a part of layer 2 header information replaced with a unique bit string." The Examiner alleged that Valencia discloses the foregoing recitation. (Final Office Action, page 3.) However, Valencia fails to teach or suggest "layer 2 header information replaced with a unique bit string." Valencia discloses no more than the use of "the Layer Two Forwarding protocol (L2F) which permits the tunneling of the link layer (i.e. HDLC, async HDLC, or SLIP frames) of higher level protocols." (Valencia, page 1.) Thus, Valencia discloses that, when creating L2F headers,

> [t]he PPP packets may be encapsulated within L2F. The packet encapsulated is the packet as it would be transmitted over a physical link.
> ...
> SLIP is encapsulated within L2F in much the same way as PPP.

(Valencia, page 10.) Note that the SLIP or PPP packets are not disclosed or suggested to be unique bit strings. Further, the packets do not replace any layer 2 header information inasmuch as they are encapsulated in the L2F header when the header is created. In short, the encapsulation disclosed by Valencia does not teach or suggest "layer 2 header information replaced with a unique bit string."

Nonetheless, the Examiner further alleged that:

> the K bit is considered to be part of the Packet key because without the K bit, the key would not be included or ignored. Therefore, the K bit is not set (i.e. is equal to 0) when no key is present and when a key is to be included the 0 is replaced with a one. Hence, part of

> the layer 2 header is replaced (0 replaced with a 1), where the 1 is considered part of the Packet Key describe in section 4.2.11 (page 14) of Valencia et al. and the remainder of the unique bit string corresponds to the key included in the header shown in the diagram on page 11.

(Final Office Action, page 9.) However, the Examiner continues to ignore the significant distinction between encapsulating a first set of data in a second set of data and replacing a first set of data with a second set of data. Valencia's disclosure of setting the K bit is merely a step in Valencia's process of generating a new L2F header and then encapsulating the payload data. The K bit is defined in Valencia's data model of the L2F header as the second bit of the header. (Valencia, page 11.) At most, Valencia discloses that the "the K bit is set in the L2F header" to signify that the "key field is present." (Valencia, page 14.) The process of encapsulation includes the instantiation of a new L2F header, including the K bit, which did not previously exist. Because a new L2F header is created, there can be no suggestion that data is replaced. The Examiner's allegation that the K bit "is replaced (0 replaced with a 1)" is therefore baseless because there is no L2F header with a K bit with value of 0 that is replaced with the value of 1. Creating a new L2F header with a K bit set to 0 or 1 cannot possibly be considered to teach or suggest "layer 2 header information replaced with a unique bit string."

Wallace does not compensate for the deficiencies of Valencia. The Examiner cited Wallace for reasons unrelated to "receiving a packet having at least a part of layer 2 header information replaced with a unique bit string." Moreover, Wallace simply describes a "validation method that uses variable personal identification numbers (PIN's)" in the context of card transactions (e.g., credit cards), and includes no teaching or suggestion of replacing, or even encapsulating, data in any manner whatsoever. (Wallace, col. 1, lines 43-44.)

Accordingly, the Section 103 rejection of claim 1, as well as the rejections of claims 2-16 and 37 depending therefrom, should be reversed for at least the foregoing reasons.

3. Claim 3 Is Patentable Over Valencia In View Of Wallace.

Claim 3 is patentable over Valencia and Wallace at least by way of its dependence from claim 1 discussed above. Additionally, claim 3 is separately patentable. For example, claim 3 recites that "the at least a part of the unique bit string examined depends on a type of the transaction." The Examiner alleged that Wallace discloses the foregoing recitation. (Final Office

Action, page 4.) However, Wallace does not in any way teach or suggest the foregoing recitation of claim 3.

Wallace simply describes a validation process that uses one or more personal identification numbers (PINs) in the context of credit card transactions (e.g., credit cards). (Wallace, col. 1, line 63 – col. 2, line 28.) In a first tier of the validation process, the system validates the proposed credit transaction based upon a static PIN. (Id.) Specifically, after receiving a PIN from a user, the system determines whether the received PIN matches a predefined PIN stored in a database. (Id.) If a match is identified, the system determines whether the credit card transaction requires a second tier of validation. (Id.) In Wallace's second validation tier, a variable PIN generated by a user-held device is provided by the user, and this variable PIN is compared to a variable PIN synchronously generated at a validation site. (Id.) If the variable PINs match, the transaction is authenticated. (Id.)

Thus, Wallace teaches the use of one or more PINs where the determination to use the second tier variable PIN, and not the content of the second tier pin, is based on criteria related to the transaction. In contrast, rather than examining two distinct PINs that are provided separately by the party according to the type of transaction, claim 3 recites that "the at least a part of the unique bit string examined depends on a type of the transaction." If, arguendo, Wallace's PIN teaches or suggests the "unique bit string," a point which Appellant does not concede, claim 3 in terms of Wallace would be analogous to receiving the PIN, but only examining part of the PIN based on transaction criteria. Wallace includes no such teaching or suggestion. Thus, Wallace does not teach or suggest the subject matter of claim 3.

Accordingly, the Section 103 rejection of claim 3 should be reversed for at least these additional reasons.

4. Claim 16 Is Patentable Over Valencia In View Of Wallace.

Claim 16 is patentable over Valencia and Wallace at least by way of its dependence from claim 1 discussed above. Additionally, claim 16 is separately patentable. For example, claim 16 recites that "the act of authenticating does not require the transmission of any authentication information from the party." The Examiner alleged that Wallace teaches the foregoing recitation. (Office Action, page 4, citing Wallace, col. 2, lines 5-29.) However, as discussed above, Wallace simply describes a validation method that uses one or more personal identification numbers (PIN's)

in the context of card transactions (e.g., credit cards). (Wallace, col. 1, line 63 – col. 2, line 28.) Specifically, Wallace discloses an interactive user process where the user must provide the PINs as user input. (Id.) In contrast, claim 16 recites that "the act of authenticating does not require the transmission of any authentication information from the party." For example, Appellant explains in his specification that:

> Although the authentication method 1022' may use just a portion(s) of the context information by itself, it is contemplated that this authentication may be used as an extension to other techniques. In this case, additional information (e.g., provided by the user and included, for example, in the data field of the packet(s)) may be examined as shown in optional block 1850. Such additional information may include a user name, a user ID, a password, etc. In optional conditional branch point 1860, it is determined whether or not the additional information matches stored information. If not, the transaction is denied as shown in block 1880. If, on the other hand, the additional information matches stored information, the transaction is approved as shown in block 1870. Note that such additional information is not required.

(Specification, page 37, line 26 – page 38, line 8, emphasis added.) Thus, a party may be authenticated by only the context information contained in the unique bit string. Wallace, in contrast, requires a party to enter a PIN, and therefore actually teaches away from the recitation of claim 16 that "the act of authenticating does not require the transmission of any authentication information from the party."

Accordingly, the Section 103 rejection of claim 16 should be reversed for at least these additional reasons.

5. Claim 33 Is Patentable Over Valencia In View Of Wallace.

Independent claim 33 recites "an input for accepting an authentication request, the authentication request including a packet having at least a part of a layer 2 header information replaced with a unique bit string" in the context of the rest of the claim. Claim 33 is patentable over the combination of Valencia and Wallace for at the same reasons as claim 1. Accordingly, the Section 103 rejection of claim 33, as well as the rejections of claims 34-36 depending therefrom, should be reversed for at least the foregoing reasons.

B. Ground of Rejection No. 2: Claims 5, 7-13, 17-24, 26-28, 30-32, and 38.

1. Claim 17 is Patentable Over Valencia and Wallace in view of Mori.

a. "determining the network ingress location from the at least a part of the unique bit string"

Independent claim 17 recites in part "determining the network ingress location from the at least a part of the unique bit string" in the context of the rest of the claim. The Examiner acknowledged that the combination of Valencia and Wallace fails to teach or suggest the foregoing recitation. (Final Office Action, page 5.) The Examiner then alleged that Mori discloses the use of location data, and that it would have been obvious to combine Mori with Valencia and Wallace in order to include information about the buyer in the transaction. (Final Office Action, page 6.)

However, Mori includes no disclosure that teaches or suggests in any way layer two headers and merely discloses the use of IP addresses with electronic transactions. (Mori, col. 14, lines 19-40.) Specifically, Mori describes an "electronic transaction process" in which an "electronic transaction procedure" is transmitted to each party to the transaction, and each party uses the procedure to perform certain steps related to an electronic transaction. (Mori, col. 2, lines 15-47.) As one example of the execution of a procedure, Mori described the sending of a message from a buyer for an "order input process." The message is described as including: "information about a buyer containing a name, address, telephone number, mail address and IP address, delivery address information (a name, address, telephone number, mail address and IP address) for the case where the address for delivery is different from that of the buyer ... and signed in a digital form by the buyer…." (Mori, col. 14, lines 13-40.)

Mori contains no discussion of "determining the network ingress location," much less determining such information "from the at least a part of the unique bit string." The Examiner makes an unjustified leap of reasoning to allege that the inclusion of an IP address in Mori's message teaches or suggests "determining the network ingress location." At most, an IP address provides one possible identifier for a particular network node. Not only are IP address assignments often subject to change, but an IP address on its own is not sufficient for "determining the network ingress location." For example, additional data would be needed to link a particular IP address to a particular "network ingress location." In other words, Mori does not include any teaching or suggestion of "determining the network ingress location."

Further, under the Examiner's reasoning, any reference that merely mentions the use of an IP address in association with an electronic transaction could be combined with the purported teachings of Valencia and Wallace to render claim 17 obvious. Clearly, the Examiner has ignored that claim 17 recites "determining the network ingress location from the at least a part of the unique bit string." Mori, simply discloses the use of an IP address with an electronic transaction. Mori is silent with respect to using the IP address as "at least a part of the unique bit string."

Accordingly, the Section 103 rejection of claim 17, as well as the rejections of claims 18-23 and 38 depending therefrom, should be reversed for at least the foregoing reasons.

b. "receiving the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string"

Claim 17 further recites in part "receiving the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string." As discussed above with respect to claim 1, the combination of Valencia and Wallace does not teach or suggest the foregoing recitation. Further, the Examiner did not cite Mori for allegedly teaching the foregoing recitation. Moreover, the addition of Mori cannot overcome the deficiencies of Valencia and Wallace at least because Mori includes no disclosure of "layer 2 header[s]." As discussed above, Mori simply discloses the use of an IP address with an electronic transaction. Thus, the combination of Valencia, Wallace, and Mori does not teach or suggest "receiving the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string."

Accordingly, the Section 103 rejection of claim 17, as well as the rejections of claims 18-23 and 38 depending therefrom, should be reversed for at least the foregoing additional reasons.

2. Claim 7 is Patentable Over Valencia and Wallace in view of Mori.

Claim 7 is patentable over Valencia and Wallace in view of Mori at least by way of its dependence from claim 1 discussed above. Additionally, claim 7 is separately patentable. For example, claim 7 recites that "the at least a part of the unique bit string examined identifies a location at which packets from the party to the transaction entered the network." For reasons discussed above with respect to claim 17, the combination of Valencia, Wallace, and Mori fails to teach or suggest the foregoing recitation.

Accordingly, the Section 103 rejection of claim 7 should be reversed for at least these additional reasons.

3. Claims 8-13 Are Patentable Over Valencia In View Of Wallace in view of Mori.

Claims 8-13 are each patentable over Valencia and Wallace in view of Mori at least by way of their dependence from claim 1 discussed above. Additionally, claims 8-13 each recite separately patentable subject matter. For example, claim 8 recites that "at least a part of the unique bit string examined identifies an individual who is a party to the transaction." Claim 9 recites that "at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs." Claim 10 recites that "at least a part of the unique bit string examined identifies a customer that is a party to the transaction." Claim 11 recites that "at least a part of the unique bit string identifies at least one of a customer identification, an individual user identification, a network ingress location, and a user class." Claim 12 recites that "at least a part of the unique bit string identifies at least two of a customer identification, an individual user identification, a network ingress location, and a user class." Claim 13 recites that "at least a part of the unique bit string identifies at least three of a customer identification, an individual user identification, a network ingress location, and a user class." The Examiner alleged that Mori's disclosure of tracking IP addresses and customer information included with electronic transactions teaches each of the foregoing recitations. (Office Action, page 6, citing Mori, col. 14, lines 19-40.)

The Examiner has not presented a factual analysis of the cited references that would result in a workable combination that would render claims 8-13 obvious, nor do the cited references render these claims obvious. Mori merely discusses customer information that may be provided with an electronic transaction. Mori is includes no teaching or suggestion related to layer 2 headers or "at least a part of the unique bit string" thereof.

Moreover, combining Mori with Valencia and Wallace would not predictably yield the subject matter of claims 8-13. For example, Mori discloses that an electronic transaction "message includes … information about a buyer containing a name, address, telephone number, mail address, and IP address, delivery address…" (Mori, col. 14, lines 19-22.) In contrast to a message that includes a name or address, claim 8 recites "at least a part of the unique bit string" which may be "examined [to identify] an individual who is a party to the transaction." Recall from claim 1 that the "unique bit string" is data that has replaced "at least a part of layer 2 header information." It would be completely unworkable to insert Mori's name and address information into a layer two

header. For example, neither the Examiner nor the references themselves, present any disclosure regarding how Valencia's L2F encapsulated data would be routable if part of the header data was replaced with Mori's customer name and address information. Thus, the combination of Valencia, Wallace, and Mori do not render claims 8-13 obvious.

Accordingly, the Section 103 rejections of claims 8-13 should be reversed for at least these additional reasons.

4. Claims 19-21 are Patentable Over Valencia and Wallace in view of Mori.

Claim 19-21 are each patentable over Valencia and Wallace in view of Mori at least by way of their dependence from claim 17 discussed above. Additionally, claims 19-21 recite separately patentable subject matter. For example, claim 19 recites that "at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs." Claim 20 recites that "at least a part of the unique bit string examined identifies a customer that is a party to the transaction." Claim 21 recites that "at least a part of the unique bit string identifies at least one of a customer identification, an individual user identification, a network ingress location, and an individual user class." The Examiner alleged that Mori's disclosure of tracking IP addresses and customer information with electronic transactions teaches each of the foregoing recitations. (Office Action, page 7, citing Mori, col. 14, lines 19-40.) However, Mori merely discloses customer information that may be included with an electronic transaction. As discussed above with respect to claims 8-13, because Mori includes no teaching or suggestion in any way related to layer 2 headers or "at least a part of the unique bit string" thereof, the combination of Valencia, Wallace, and Mori fails render the foregoing claim recitations obvious.

Accordingly, the Section 103 rejections of claims 19-21 should be reversed for at least these additional reasons.

5. Claim 24 is Patentable Over Valencia and Wallace in view of Mori.

a. "layer 2 header information replaced with a unique bit string . . ."

Independent claim 24 recites in part "receiving the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string." As discussed above with respect to claim 1, the combination of Valencia, Wallace, and Mori fails to teach or suggest the foregoing recitation.

Accordingly, the Section 103 rejection of claim 24, as well as the rejections of claims 26 and 27 depending therefrom, should be reversed for at least the reasons stated above with respect to claim 17.

b. "the unique bit string uniquely identifies the party and an ingress location of the network . . ."

Claim 24 further recites in part that "the unique bit string uniquely identifies the party and an ingress location of the network, and [that] no information in addition to the unique bit string is needed for authenticating the party to the transaction." As an initial matter, the Examiner failed to address the second portion of the foregoing recitation. Specifically, the Examiner made no allegations regarding how the cited references teach or suggest "[that] no information in addition to the unique bit string is needed for authenticating the party to the transaction." In addition, as discussed above with respect to claim 17, the cited references do not teach or suggest that that "the unique bit string uniquely identifies the party and an ingress location of the network." Specifically, Mori's IP address, which is not included in a layer two header, does not "uniquely [identify] the party and an ingress location of the network."

Accordingly, the Section 103 rejection of claim 24, as well as the rejections of claims 26 and 27 depending therefrom, should be reversed for at least these additional reasons.

6. Claim 27 is Patentable Over Valencia and Wallace In View Of Mori.

Claim 27 is patentable over Valencia and Wallace in view of Mori at least by way of its dependence from claim 24 discussed above. Additionally, claim 27 is separately patentable. For example, claim 27 recites that "the unique bit string identifies a logical port at which the packet entered the network." As discussed above with respect to claim 17, the combination of Valencia, Wallace, and Mori fails to teach or suggest "determining the network ingress location from the at least a part of the unique bit string." Nor do the references discuss identifying "a logical port" at all. Accordingly, the cited references clearly fail to teach or suggest that "the unique bit string identifies a logical port at which the packet entered the network."

Accordingly, the Section 103 rejection of claim 27 should be reversed for at least these additional reasons.

7. Claim 28 Is Patentable Over Valencia And Wallace In View Of Mori.

Independent claim 28 recites "applying a unique bit string to layer 2 header information of packets entering the network, the unique bit string uniquely identifying the party and an ingress location of the network" in the context of the rest of the claim. Claim 28 is patentable over the combination of Valencia and Wallace in view of Mori for at the reasons set forth above concerning claim 17. For example, claim 28 recites "the unique bit string uniquely identifying the party and an ingress location of the network." As discussed above with respect to claim 17, Mori merely discloses the use of IP addresses with electronic transactions. Such use of an IP address clearly does not teach or suggest the foregoing recitation.

Accordingly, the Section 103 rejection of claim 28, as well as the rejections of 30-32 depending therefrom, should be reversed for at least the reasons stated above with respect to claim 17.

8. Claim 31 is Patentable Over Valencia and Wallace In View Of Mori.

Claim 31 is patentable over Valencia and Wallace in view of Mori at least by way of its dependence from claim 28 discussed above. Additionally, claim 31 is separately patentable. For example, claim 31 recites that "the unique bit string identifies a logical port at which the packet entered the network." As discussed above with respect to claim 17, the combination of Valencia, Wallace, and Mori fails to teach or suggest "determining the network ingress location from the at least a part of the unique bit string." Accordingly, the cited references clearly fail to teach or suggest that "the unique bit string identifies a logical port at which the packet entered the network."

Accordingly, the Section 103 rejection of claim 31 should be reversed for at least these additional reasons.

9. Claim 32 is Patentable Over Valencia and Wallace in view of Mori.

Claim 32 is patentable over Valencia and Wallace in view of Mori at least by way of its dependence from claim 28 discussed above. Additionally, claim 32 is separately patentable. For example, claim 32 recites that "no information in addition to the unique bit string is needed for authenticating the party to the transaction." The Examiner alleged that Wallace teaches the foregoing recitation. (Office Action, page 8, citing Wallace, col. 2, lines 5-29.) However, as discussed above, Wallace simply describes a validation method that uses one or more personal

identification numbers (PIN's) in the context of card transactions (e.g., credit cards). (Wallace, col. 1, line 63 – col. 2, line 28.) Moreover, Wallace does not teach or suggest that the PIN be included as "the unique bit string" of a layer 2 header.

Accordingly, the Section 103 rejection of claim 31 should be reversed for at least these additional reasons.

10. Claim 38 is Patentable Over Valencia and Wallace in view of Mori.

Claim 38 is patentable over Valencia and Wallace in view of Mori at least by way of its dependence from claim 17 discussed above. Additionally, claim 38 is separately patentable. For example, claim 38 recites that "the layer 2 header information is a MAC header." The Examiner rejected claim 38 by citing references "Nguyen" and "DLL" not previously identified in the Final Office Action. The rejection of claim 38 should be reversed at least because no clear basis for rejection is set forth. Further, Appellant submits that the combination of Valencia, Wallace, and Mori fails to teach or suggest any subject matter related to MAC headers, much less the foregoing recitation.

Accordingly, the Section 103 rejection of claim 38 should be reversed for at least these additional reasons.

VIII. CONCLUSION

In view of the foregoing arguments, Appellant respectfully submits that the pending claims are novel over the cited references. The Examiner's rejections of all pending claims are improper because the cited references of record do not teach or suggest each and every element of the claimed invention. In view of the above analysis, a reversal of the rejections of record is respectfully requested of this Honorable Board. It is believed that any fees associated with the filing of this paper are identified in an accompanying transmittal. However, if any additional fees are required, they may be charged to Deposit Account 18-0013, under Order No. 65632-0560, from which the undersigned is authorized to draw. To the extent necessary, a petition for extension of time under 37 C.F.R. 1.136(a) is hereby made, the fee for which should be charged against the aforementioned account.

Respectfully submitted,

Dated: June 10, 2008

Electronic signature: /Jeffrey T. Gedeon/
Jeffrey T. Gedeon
Registration No.: 57,510
Charles A. Bieneman
Registration No.: 51,472
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 25537
Attorneys for Appellant

IX. CLAIMS APPENDIX

Pursuant to 37 CFR § 41.37(c)(1)(viii), the following listing provides a copy of the claims involved in the appeal.

1. A method for authenticating a party to a transaction, the method comprising:

receiving a packet having at least a part of layer 2 header information replaced with a unique bit string;

examining at least a part of the unique bit string;

comparing the at least a part of the unique bit string examined with stored information; and

authenticating the party only if the at least a part of the unique bit string examined matches the stored information.

2. The method of claim 1 further comprising:

approving a transaction if the party was authenticated.

3. The method of claim 1 wherein the at least a part of the unique bit string examined depends on a type of the transaction.

4. The method of claim 2 wherein the stored information compared with the at least a part of the unique bit string examined depends on the type of the transaction.

5. The method of claim 3 wherein the type of the transaction is selected from a group of transaction types consisting of: (A) transactions greater than a predetermined amount; (B) transactions less than a predetermined amount; (C) purchases delivered to a credit card billing address; and (D) purchases delivered to an address other than a credit card billing address.

6. The method of claim 1 wherein the stored information compared with the at least a part of the unique bit string examined depends on a type of the transaction.

7. The method of claim 1 wherein the at least a part of the unique bit string examined identifies a location at which packets from the party to the transaction entered the network.

8. The method of claim 1 wherein the at least a part of the unique bit string examined identifies an individual who is a party to the transaction.

9. The method of claim 1 wherein the at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs.

10. The method of claim 1 wherein the at least a part of the unique bit string examined identifies a customer that is a party to the transaction.

11. The method of claim 1 wherein the at least a part of the unique bit string identifies at least one of a customer identification, an individual user identification, a network ingress location, and a user class.

12. The method of claim 1 wherein the at least a part of the unique bit string identifies at least two of a customer identification, an individual user identification, a network ingress location, and a user class.

13. The method of claim 1 wherein the at least a part of the unique bit string identifies at least three of a customer identification, an individual user identification, a network ingress location, and a user class.

14. The method of claim 1 wherein the unique bit string is provisioned by a network service provider.

15. The method of claim 1 wherein the unique bit string is controlled by a network service provider.

16. The method of claim 1 wherein the act of authenticating does not require the transmission of any authentication information from the party.

17. A method for tracking a network ingress location at which a packet associated with a transaction originated, the method comprising:

receiving the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string;

examining at least a part of the unique bit string; and

determining the network ingress location from the at least a part of the unique bit string.

18. The method of claim 17 wherein the at least a part of the unique bit string examined identifies an individual who is a party to the transaction.

19. The method of claim 17 wherein the at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs.

20. The method of claim 17 wherein the at least a part of the unique bit string examined identifies a customer that is a party to the transaction.

21. The method of claim 17 wherein the at least a part of the unique bit string identifies at least one of a customer identification, an individual user identification, a network ingress location, and an individual user class.

22. The method of claim 17 wherein the unique bit string is provisioned by a network service provider.

23. The method of claim 17 wherein the unique bit string is controlled by a network service provider.

24. A method for authenticating a party to a transaction, the method comprising:

receiving a packet having at least a part of layer 2 header information replaced with a unique bit string;

examining at least a part of the unique bit string;

comparing the at least a part of the unique bit string examined with stored information; and

approving a transaction only if the at least a part of the unique bit string examined matches the stored information,

wherein the unique bit string uniquely identifies the party and an ingress location of the network, and no information in addition to the unique bit string is needed for authenticating the party to the transaction.

25. (Cancelled)

26. The method of claim 24 wherein the unique bit string is maintained as the packet is communicated within the network.

27. The method of claim 24 wherein the unique bit string identifies a logical port at which the packet entered the network.

28. A method for authenticating a party to a transaction, the method comprising:

a) applying a unique bit string to layer 2 header information of packets entering the network, the unique bit string uniquely identifying the party and an ingress location of the network;

b) examining at least a part of the unique bit string;

c) comparing the at least a part of the unique bit string examined with stored information; and

d) approving a transaction only if the at least a part of the unique bit string examined matches the stored information.

29. (Cancelled)

30. The method of claim 28 wherein the unique bit string is maintained as the packet is communicated within the network.

31. The method of claim 28 wherein the unique bit string identifies a logical port at which the packet entered the network.

32. The method of claim 28 wherein no information in addition to the unique bit string is needed for authenticating the party to the transaction.

33. An apparatus for authenticating a party to a transaction, the apparatus comprising:

a) an input for accepting an authentication request, the authentication request including a packet having at least a part of a layer 2 header information replaced with a unique bit string;

b) storage means for storing authentication information;

c) means for examining at least a part of the unique bit string;

d) a comparison facility for comparing the at least a part of the unique bit string examined with the stored authentication information; and

e) means for authenticating a party to a transaction only if the at least a part of the unique bit string examined matches the stored authentication information.

34. The apparatus of claim 33 further comprising:

f) means for approving the transaction if the party was authenticated.

35. The apparatus of claim 33 further comprising:

f) an output for forwarding an authentication response to the transaction facility.

36. The apparatus of claim 34 further comprising:

g) an output for forwarding an authorization response to the transaction facility.

37. The method of claim 1, wherein the layer 2 header information is one of data link layer header and a network access layer header.

38. The method of claim 17, wherein the layer 2 header information is a MAC header.

X. EVIDENCE APPENDIX

(Not applicable.)

XI. RELATED PROCEEDINGS APPENDIX

(Not applicable.)